PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-134482
(43)Date of publication of application : 09.05.2003

(51)Int.Cl. H04N 7/08
G09C 5/00
H04L 9/10
H04N 7/081

(21)Application number : 2002-201275 (71)Applicant : EASTMAN KODAK CO
(22)Date of filing : 10.07.2002 (72)Inventor : JONES PAUL W

(30)Priority
Priority number : 2001 902345 Priority date : 10.07.2001 Priority country : US

(54) SYSTEM FOR SECURE WATERMARKING OF DIGITAL IMAGE SEQUENCE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a digital movie watermarking system for providing security over all the aspects of a watermarking process in order to ensure an embedded watermark and the integrity of information represented by the embedded watermark.
SOLUTION: A system and method for securely embedding a watermark representing message data into movie data consisting of one or more frames of a digital image sequence, and displaying one or more frames of the digital image sequence containing the embedded watermark, includes providing a secure environment; combining the movie data with the watermark within the secure environment to produce watermarked movie data; and forming a displayed image from the watermarked movie data within the secure environment.

LEGAL STATUS

[Date of request for examination] 11.05.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] To the movie data which consist of one or more frames of a digital image sequence The means for being the system which displays one or more frames of the digital image sequence which embeds the watermark showing message data safely and includes the embedded watermark, and offering a safe environment, In order to generate the movie data into which the watermark was put, the means for combining with movie data and a watermark within an insurance environment, and within an insurance environment It carries out and is [safe ** of the digital image sequence characterized by including the means for forming the displayed image from the movie data into which the watermark was able to be put, or] a system.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Generally this invention relates to the field of digital image processing, and the system for embedding a watermark within an insurance environment especially at a digital image sequence.

[0002]
[Description of the Prior Art] It is the purpose which proves ownership, pursues the origin of data carrying out in digital **, and prevents an unauthorized copy, or conveys the additional information (metadata) about the contents, and means embedding the message hidden in the image or the image sequence. It is a far-reaching product including a digital still camera, a digital video camera, a printer, other hard copy output equipments, and contents delivery service (for example, photograph finishing of the Internet base) to put in a watermark, and it may be used. In recent years, there is a remarkable interest in the electronic distribution and the display of a theatrical film which are called a digital movie theater. This can be given to studio or a distribution contractor by the thing which protects the contents of a movie from unauthorized use and for which the source of the contents which proved ownership and were stolen there being powerful needs and spacing is followed (letting use of the stamp of the hidden date / time amount / location inserted at the time of movie distribution and/or a presentation pass). Although it relates to especially this invention putting a watermark into an image sequence, it is carried out in this way and has usefulness in application like a digital movie theater.
[0003] The method of putting in many watermark is described in the advanced technology containing a patent or technical reference. Many of these approaches are carried out in "multimedia ** of Hartung and Kutter, and it is described by "a consciousness watermark for a digital image and video" besides technical", Proc.IEEE, 87(7) pp.1079-1107 (1999), and Wolfgang, Proc.IEEE, and review document like 87(7) pp.1108-1126 (1999).
[0004] The radical difference of various approaches is to any a watermark shall be applied between a space field or a frequency domain. It carries out in space ******, a technique adds a watermark pattern to the pixel value of a direct digital image, it carries out in ********** to it, and a technique is added to the transform coefficient (for example, discrete cosine conversion (DCT) multiplier used for a JPEG and MPEG-compression image) which expresses a digital image for a watermark pattern. There are U.S. Pat. No. 6,044,156 published [else / Honsinger] on March 28, 2000 and U.S. Pat. No. 5,636,292 published to Rhoads on June 3, 1997 in the example of the space field technique in the advanced technology. There are U.S. Pat. No. 5,809,139 published [else / Girod] on September 15, 1998, U.S. Pat. No. 5,901,178 published [else / Lee] on May 4, 1999, and U.S. Pat. No. 5,930,369 published [else / Cox] on July 27, 1999 in the example of the frequency-domain technique in the advanced technology.
[0005] space field approach -- be -- a frequency-domain approach -- be -- most techniques were spaced and use the pseudo-random noise (PN) sequence (or two or more sequences) for extract processing. PN sequence is used as a carrier signal generally modulated with message data, and it serves as distributed message data (namely, watermark pattern) which cross many pixels or transform coefficients and are distributed as a result. This key must be known, when extracting the original

message data which spaced and were connected with it although a secret key (namely, seed value) is generally used in case PN sequence is generated. As an environment where a watermark is put in for a digital cinema system, it is desirable that the movie embeds a watermark during a plan. Thereby, unique presentation information (a theater, a specific screen, a time stump, etc. are shown) can be included in the embedded watermark. When a movie is copied unlawfully, the unique presentation information (known as a "fingerprint") which shows larcenous time amount and a larcenous location can be extracted from the watermark embedded to the copy like all the information on the others contained in the watermark. When such information is used in legal procedure, it needs to be shown that information should fail to be what kind of form.

[0006] In a typical movie theater, many people may access the contents of a movie, and projection equipment. Although this is not employed by the owner of a theater, a projectionist, a maintenance staff, and the theater, it also contains the individual in whom unauthorized access is possible. Since access to the digital data showing the contents of a movie can be copied easily without quality degradation, this is a serious problem. In order to prevent this, it is understood well that digital cinema data must be protected with powerful encoding technology. To a secret key, although based on a public key infrastructure (PKI), it lets the security protocol [like] known well pass, and such a technique requires decode of the encryption data which can be sent at a theater at insurance. Encryption and extensive description of a security protocol are an "application code handbook" and CRC. Press, Boca Raton, and floor line1997 and ISBN 0-8493-8523-7 see. [/ else / Menezes]

[0007]

[Problem(s) to be Solved by the Invention] When putting a watermark into digital cinema data, the secret key which puts in a watermark offers a certain amount of safety required for an extract at least as space. A watermark key can be sent to the theater using the same insurance method as being used for a decode key. However, it is a digital cinema system and cannot be said to be enough to control only a watermark key (or two or more keys). Since many people may be accessible to various components of a digital cinema image processing system, it is necessary to provide with safety all the potential points about which it will be apprehensive if it spaces and the sound condition of a process receives damage.

[0008] Therefore, in order to secure the integrity of the embedded watermark and the information which it expresses in this way, it spaces, safety is offered covering all the fields of a process, digital cinema **** is carried out, and the system is needed.

[0009]

[Means for Solving the Problem] This request is filled by this invention. This invention to the movie data which consist of one or more frames of a digital image sequence Embed the watermark showing message data safely and include the

embedded watermark further. The system and approach of displaying one or more frames of a digital image sequence are offered, and it offers an insurance environment.; in order to create the movie data into which the watermark was put It includes forming a display image from the movie data into which the watermark was able to be put within combining–within insurance environment–movie data and watermark;, and an insurance environment.

[0010] This invention offers the improved safety, while embedding a watermark by the digital image sequence, in order to secure the justification of the information included in such a watermark. Moreover, it offers updating safely the important parameter into which it is put as a watermark like a key and/or a message, and recording these updated parameters on insurance.

[0011]

[Embodiment of the Invention] As mentioned above, a secret watermark key (there may be plurality) can be protected during delivery using the encoding technology known well and a security protocol. However, it may be desirable for the frame of the number of specification in a movie sequence to pass, and to change all or a part of root key, in order to offer the safety strengthened with the digital cinema system, and/or in order to make the visibility of a watermark pattern into min (the cognition not changing space and according from a pattern to an appreciation person is difficult for changing a pattern). The thing of key generation accompanied by some control at least also has the capacity to correct a key, within a local theater environment. Such correction of a key must be made by the safe approach, and further, probably, it needs to detect use of a key safely, in order to perform a next extract.

[0012] However, in a digital cinema system, it cannot be said that it is enough only by controlling a watermark key. It is also required to protect watermark message data. It is because any alterations of message data may become the cause of making incorrectness identifying a theater and/or time amount when message data are extracted from an illegal copy. Furthermore, it may be desirable to correct message data so that renewal of a time amount code may be made after several specification. Probably, it will also be required for insurance to detect message use.

[0013] At the end, after putting in spaces, it is necessary to offer safety for digital cinema data. Even if, though already put into the watermark of unique information by digital cinema data, a secondary watermark (different information from an original watermark is included) may be similarly embedded to them. Since it becomes impossible [solving which watermark is the first watermark] ("deadlock" problem), it will smash the certainty of a watermark of original in any legal procedure.

[0014] Safety is attained by spacing within an insurance environment and performing a process by this invention. An unauthorized individual is a meaningful approach and means that the information in which the arbitration of a process was stored or the input of arbitration, an output, or internal connection cannot be accessed as an insurance environment. This prevents an unauthorized individual's acquiring the

process which puts in a watermark, and the information about the parameter, and/or affecting it. Even if it is the case where data are having the watermark already embedded even if, it prevents gaining the digital data showing a movie again.
[0015] A safe environment is finished through physical and using a logical protection technique. An easy physical protection technique is putting all system components and the related information of arbitration on the locked room which can be accessed only in a suitable key or suitable combination. Similarly, the system component was able to be contained in tough physical housing which resists an alteration by the (it is (like the case of hardened steel with the locked lid)) mechanical property.
[0016] When there is an alteration, housing can cut a power source and can contain the lid switch which eliminates a still more important logged point, and other safety devices again. The further physical safety can be offered using the circuit designed so that it might especially become impossible operating it, no matter the hi-technology approach like a semiconductor chip and alteration [what] may take place. Some arguments on these hi-technology security treatment are "a tamper resistance-admonition comment" and The. Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, CA, Nov.1996, pp.1-11, and ISBN 1-880446-83-9 see. [/ else / Anderson] However, in a digital cinema system, from one physical location, seemingly the information on some needs to be transmitted to somewhere else, and must give suitable protection to this information by the logical approach. For example, the digital data showing a movie must be transmitted from a distribution site to each theater. And as mentioned above, this data can be protected using the powerful encryption approach and a security protocol.
[0017] safe -- digital cinema **** is carried out and the fundamental configuration of a system is shown in drawing 1 . The remote data server 10 (for example, distribution site) is compressed, and delivers the enciphered movie data to a theater. Although a movie is compressed within the limits of constraint of a current technique in order to realize a more effective transfer of data, compression is not essential to an operation of this invention. Compressed data is enciphered in order to prevent an unauthorized individual accessing digital cinema data between the deliveries to a theater. The remote decode key server 12 delivers a safe decode key (or two or more keys) to a theater, in order to decode the enciphered movie data. In some system, the remote data server 10 and the remote decode key server 12 may be contained in the single server. In the alien system, the remote data server was able to be replaced with another means, in order to deliver movie data to physical storing media like a theater, for example, a DVD disk.
[0018] It is compressed at a theater and the data and the decode key which were enciphered are sent to the decode unit 14. In order to generate the compression movie data which are not enciphered using a decode key, a decode unit is compressed and decodes the enciphered data. The compressed movie data are sent to the decompression unit 16 in order to generate incompressible movie data from it. Incompressible movie data express the sequence of one or more frames of digital

data. Each frame is shown as a frame n (n= 1, 2, ..., N). N is the total of the frame of a movie sequence here.

[0019] In order to generate movie data including a watermark, the incompressible digital data for each frame spaces digital cinema data, they are combined with a pattern, and it spaces them, and is sent to a unit 18. A watermark pattern can be generated using the approach with which many differ, and can also change a watermark pattern after the frame of the number of specification so that it may be stated immediately henceforth. Although it may be necessary to put a watermark into each frame, generally the frame of a considerable number will contain a watermark pattern at least.

[0020] The movie data into which the watermark was able to be put are sent to the image formation assembly 20 which changes digital data into the visible image by the audience of a theater which can be appreciated from it. A result is the projection frame n including the watermark embedded within the limits of the displayed contents of a movie. When a pirate edition video contractor makes the unauthorized copy of the projected movie, a watermark can be behind extracted, in order to be conveyed with a copy and to show information about the movie like the location of an illegal copy, and time amount.

[0021] In the desirable example of this invention, it is contained the decode unit 14, the decompression unit 16, and in the insurance environment of the theater where a unit 18 and the image formation assembly 20 are altogether shown in drawing 1 by spacing. It means that this means that an unauthorized individual cannot access decode data, decompression-device rest data, or the data into which the watermark was put, and still such a person can space it, and it can affect the information about a process, or cannot be obtained. The single Physical Unit generally called a "projector" can be provided with a safe environment by unifying all these processing units. The projector contains sufficient physical insurance policy for preventing the internal configuration element of arbitration, or unauthorized access to a connection. These policies can include the invasion-detecting circuit which makes a component actuation impossible, when it acts as the monitor of anti-(it is (like case of locked steel)) alteration housing, and/or the integrity of an overall system and unauthorized access is made. In order to space and to protect a decode process, an invasion-detecting circuit may delete various logged points like a key register and a message register again, when integrity of a system is made dangerous.

[0022] the desirable example described now -- decode and decompression -- it spaces, and all image formation processes are put together and made into the single insurance unit. However, probably, it will also be useful to divide these processes into two or more Physical Units connected by safe logical connection. As shown in drawing 2 , the decode unit 14 and the decompression unit 16 are held in one safe Physical Unit, and, on the other hand, are spaced, and a unit 18 and the image formation assembly 20 may be held in other safe Physical Units. These two insurance units are connected using a safe local communication link, and the safety

is offered by powerful encryption / decompression protocol, for example. The safe Physical Unit which spaces and includes a unit 18 and the image formation assembly 20 constitutes a projector from this system. Moreover, it is also possible to finish setting up other configurations of the safe Physical Unit accompanied by a safe local communication link, and it includes spacing through the separated Physical Unit accompanied by the safe local communication link to the image formation assembly 20 from the decompression unit 16, and arranging equipment 18.

[0023] It is combined with the incompressible movie data for the frame n through which it spaced and to which the watermark was given in the system with safe drawing 1 . As mentioned above, this watermark combination process can be made in a space field or a frequency domain. However, in other examples of this invention, a watermark combination process is applied to the compressed data for Frame n. Compression technology like MPEG and JPEG essentially includes frequency disassembly of original image data, therefore they can offer the convenient framework for performing frequency-domain watermark ON **. drawing 3 is spaced through compressed data and ON ** is performed -- safe -- it spaces and a system is shown. In this system, it is compressed, and the enciphered movie data are sent to the decode unit 14 from the remote data server 10, and the remote decode key server 12 offers a decode key safe for a decode unit. The decode unit 14 generates compression movie data, in order that compression movie data may generate compressed data including a watermark after that, it is spaced, is spaced in a unit 18 and combined with a pattern. The data into which it was compressed into and the watermark was able to be put are sent to the decompression unit 16 from it, and generate the movie data into which the watermark was able to be put there, i.e., incompressible movie data including a watermark. The movie data into which the watermark was able to be put are sent to the image formation assembly 20 which changes digital data into the visible image which an audience can appreciate at a theater. In this system, they may be decode, decompression, and a Physical Unit with plurality safe [to which it spaced through, and the image generation process was again included in the insurance environment, and it was connected by the single safe Physical Unit or the safe communication link].

[0024] It spaces, and is compressed in a system and the enciphered data with safe drawing 13 are directly sent to the decode unit 14 from the remote data server 10. This means real-time transmission of movie data. It is desirable for it to be compressed for next playback and to have the local theater server which stores the enciphered data in many systems. Then [delivery and], in drawing 4 , this configuration is shown, the remote data server 10 is compressed and data are stored in the local theater server 22 in preparation for next use in the enciphered data here. While compression is not indispensable for this invention, it is used by many systems by the request for delivery of efficient storing and movie data. However, encryption is a component required in order to protect data from unauthorized access, and when it is saved at a local theater server, it may be unable

to be called completely safe environment. When a movie is shown, the local theater server 22 is sent to the decode unit 14 which uses a decode key, in order to generate the movie data which were compressed and were compressed in the enciphered data. As stated for the system of drawing 1 , a deconstructivism press is carried out by the decompression unit 16, compressed data spaces, in order to space further and to generate entering movie data, and a watermark pattern is combined with the movie data by which the deconstructivism press was carried out using equipment 18. The movie data into which the watermark was able to be put are sent to the image formation assembly 20 which makes the visible image which had the watermark embedded after that. again -- decode and decompression -- it spaces and the image formation unit is contained in the insurance environment.
[0025] Probably, it will also be useful to move a local theater server into an insurance environment. As shown in drawing 5 , this configuration is compressed, the enciphered movie data are made to decode by the decode unit 14, and the compression movie data produced as a result are stored in the local theater server 22 from it. Since the local theater server 22 is contained in the insurance environment, access to the data by the unauthorized individual is prevented, and compressed data can be stored in the format of not enciphering. When a movie is announced, delivery and the incompressible movie data obtained as a result space through the decompression unit 16 from it the movie data with which the local theater server was compressed, a watermark can be put in by the unit 18, and it is displayed using the image formation assembly 20. Moreover, arrangement of a local theater server can be attained after the decode unit 14 and the decompression unit 16. In that case, the local theater server 22 stores the decoded incompressible movie data in an insurance environment. About a memory requirement, while this system is inefficient, it simplifies the executive operation to movie data at the presentation time. It is far easier to carry out it at once for every movie show, rather than it repeats decode and decompression.
[0026] It is shown in drawing 15 described now, and spaces, and a watermark pattern is spaced and it enables it to use a unit 18 in a system. This pattern can include the information which spaces, can preset to a unit, spaces and expresses unique ID of a unit and/or a projector at the time of manufacture. However, it was restricted very much and, as for this approach, correcting a watermark pattern repeatedly the sakes [following] makes min the visibility of; which updates;2 watermark information that the additional safety to desirable :1 watermark information is offered (for example, since time stamp information is reflected), and the watermark pattern to 3 theater audience. In other desirable examples of this invention, a watermark pattern is corrected by changing a watermark key and/or a watermark message at various points of the sequence of a movie frame. As shown in drawing 6 , the watermark pattern of presetting is exchanged by the watermark pattern generation equipment 24 which spaces from watermark key generation equipment 26, spaces a key from watermark message generation equipment 28, and receives a message. watermark

pattern generation equipment 24, key generation equipment 26, and message generation equipment 28 -- and it spaces and a unit 18 is altogether contained in an insurance environment. As mentioned above, it was possible for you to have been made to exist by two or more Physical Units which equipped these safe communication link to which it spaces, and the insurance environment for a component can be constituted in a single Physical Unit (this may contain alien-system components, such as the image formation assembly 20), or it spaces through, and a component conveys data between Physical Units. For example, it can include in the Physical Unit into which watermark pattern generation equipment 24, key generation equipment 26, and message generation equipment 28 could be included in one Physical Unit (it may be in a theater or you may be in a remote site), and equipment 18 was divided by spacing.

[0027] A watermark key and/or a watermark message are correctable throughout the sequence of a movie frame using the system shown in drawing 6 , if there is a demand. For example, in the case of m>=1, a watermark key can also change a key by the random approach within the limits of watermark key generation equipment 26 that it can change every m frames. Since the key must become clear in order to extract a watermark, it will be useful to use only the key from which the limited number differs. It is easy to perform a thorough search of a different key between next watermark extract processes using a limited number of keys. By changing a watermark key, the knowledge of the key used for one frame stops offering no knowledge about the key used for other frames, will space, and will provide a process with the further safety. In addition, use of most keys which space and are different with a technique brings about a completely different watermark pattern. This prevents that an individual has a watermark pattern specified by what (for a changeless watermark pattern to be reinforced while spoiling the contents of an image with a motion) a multiple frame is averaged for. Furthermore, the watermark pattern which changes through time amount will not be more unpleasant than/which is harder to be found for the appreciation person of the audience of a theater.

[0028] Similarly, a watermark message can be changed for every frames of each movie sequence, or a fixed number of frames of a sequence within the limits. Like time amount or a day entry, especially a watermark message can correct unique ID of a theater specification screen etc. so that specific presentation information may be included. Furthermore, a hour entry can be updated through the sequence of a movie frame, consequently when it is m>=1, a new time stamp can be contained in watermark information every m frames. In order to offer sufficient justification for a time amount stamp, watermark message generation equipment 28 can contain a perfect time recorder within an insurance environment. An unauthorized individual cannot correct a time recorder in a movie data-processing path, without making one or more required components into use impossible.

[0029] Watermark pattern generation equipment 24 needs to turn cautions to the point which needs to generate a new watermark pattern, only when a watermark key

or a watermark message changes. When watermark pattern generation equipment can act as the monitor of the key offered with watermark key generation equipment 26 and watermark message generation equipment 28, and the message, respectively and a key or a message is corrected, a new watermark pattern is generated. Moreover, it is possible to use the watermark pattern of the number of limitation which calculated beforehand and was stored in memory within the limits of watermark pattern generation equipment 24. In this case, a watermark key and a message commit the address in a look-up table, and a corresponding watermark pattern is taken out from memory.

[0030] In other desirable examples of this invention, the watermark key generated with watermark key generation equipment 26 and the watermark message generated with watermark message generation equipment 28 are transmitted to insurance at the remote watermark database 30. As shown in drawing 7 , since the watermark key generated with watermark key generation equipment 26 is stored and use of the watermark information extract from the unauthorized copy of movie data is presented with it later, it is sent to the remote watermark database 30 via a safe communication link. The safe communication link was able to be offered using the encryption approach and protocol which were known well. In a watermark database, each watermark key may relate to a specific frame or two or more frames from a given movie and specific specific theater/screen, and/or a show. However, it may be enough as it just to record the key used again for specific theater / screen without relation with a specific frame or two or more frames, and the movie show or two or more keys. Similarly, with a safe means, the watermark message generated with watermark message generation equipment 28 is sent to the remote watermark database 30, and can be connected with a specific frame or a series of frames and/or specific specific theater/screen, and a show there. If a watermark key and a message are stored in an encryption format in the remote watermark database 30 or the database itself is contained in an insurance environment, it can save in the decoded format.

[0031] In another example with desirable this invention, all or a part of watermark key and/or watermark message are offered by the remote watermark server. As shown in drawing 8 , the remote watermark server 32 sends a watermark root key to the watermark key generation equipment 26 which exists in an insurance environment at insurance. When a root key is only a partial key, watermark key generation equipment 26 adds a suffix and/or a prefix to a root key, in order to make a perfect key. Or a remote server is able to send the perfect key which spaces without being corrected after that and sent to pattern generation equipment. It can use as an initialization key which also spaces a perfect key behind and by which it is corrected with key generation equipment 26. The remote watermark server 32 can send many root keys again, and each root key in this case is connected with the sequence of the specific frame in a movie, or a multiple frame.

[0032] Similarly, the remote watermark server 32 is spaced through insurance, and

sends a root message to the watermark message generation equipment 28 which exists in an insurance environment. A root message can include the unique presentation ID for the show of the specification of a movie, including a specific theater and unique ID of a screen. Watermark message generation equipment 28 was able to add the time stamp to unique ID after that. Here, in case a time stamp shows a movie, it is updated at various points. As for a root message, it is possible for it to be a perfect message (or a series of messages) including a theater and a hour entry again.

[0033] The safety of a watermark root key and a root message is offered during a transfer by the encryption approach and protocol which were known well. Furthermore, before they are delivered at a theater, in order for a remote watermark server to prevent an unauthorized individual altering a root key or a message, it is protected in the insurance environment. The remote watermark server is also maintaining the safe database to which a watermark root key and a root message are related with a specific movie frame or a series of frames and/or specific specific theater/screen, and a show.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] In a digital cinema system, it is drawing showing the system for embedding a watermark to movie data within an insurance environment.

[Drawing 2] In a digital cinema system, it is drawing showing another system for embedding a watermark to movie data within an insurance environment.

[Drawing 3] In a digital cinema system, it is drawing showing the system for embedding a watermark to the movie data compressed within the insurance environment.

[Drawing 4] In the digital cinema system accompanied by the local storage of the enciphered data and the compressed data, it is drawing showing the system for embedding a watermark within an insurance environment.

[Drawing 5] In the digital cinema system accompanied by the local storage of the enciphered data and the compressed data, it is drawing showing the system for embedding a watermark within an insurance environment.

[Drawing 6] It is drawing showing the system for embedding a watermark within an insurance environment in the spacing and using key and watermark message digital cinema system generated locally.

[Drawing 7] It is drawing showing the system for embedding a watermark within an insurance environment in the digital cinema system accompanied by [space and] the remote database storage of a key and a watermark message generated locally.

[Drawing 8] In the digital cinema system using the safe watermark root key and watermark root message which are generated by the remote watermark server, it is drawing showing the system for embedding a watermark within an insurance environment.

[Description of Notations]

10 A remote data server, 12 A remote decode key server, 14 decode unit, 16 A decompression unit, 18 It spaces and is a unit and 20. An image formation assembly, 22 A local theater server, 24 It spaces and is pattern generation equipment and 26. It spaces and is key generation equipment and 28. It spaces and is message generation equipment and 30. A remote watermark database, 32 Remote watermark server.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－134482
（P2003－134482A）
(43)公開日　平成15年５月９日(2003.5.9)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｎ　7/08		Ｇ０９Ｃ　5/00		５Ｃ０６３
Ｇ０９Ｃ　5/00		Ｈ０４Ｎ　7/08	Ｚ	５Ｊ１０４
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	
Ｈ０４Ｎ　7/081				

審査請求　未請求　請求項の数１　ＯＬ　（全 11 頁）

(21)出願番号　特願2002－201275(P2002－201275)

(22)出願日　平成14年７月10日(2002.7.10)

(31)優先権主張番号　０９／９０２３４５

(32)優先日　平成13年７月10日(2001.7.10)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000846
イーストマン　コダック　カンパニー
アメリカ合衆国，ニューヨーク14650，ロチェスター，ステイト　ストリート343

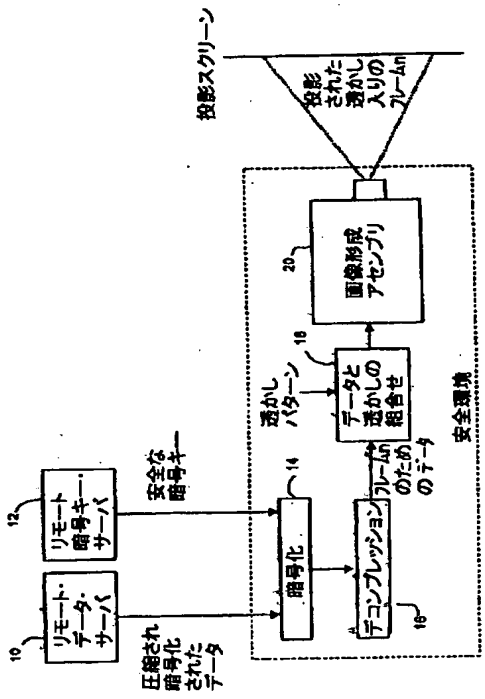
(72)発明者　ポール・ダブリュー・ジョーンズ
アメリカ合衆国14428ニューヨーク州チャーチヒル、リード・ロード644番

(74)代理人　100062144
弁理士　青山　葆　（外１名）

Ｆターム(参考)　5C063 AB06 CA29 CA36 DA13
5J104 AA01 AA08 AA12 AA14 NA02
NA42

(54)【発明の名称】　デジタル画像シーケンスの安全透かし入れシステム

(57)【要約】
【課題】　埋め込まれた透かしと、それが表す情報の完全性を確保するために、透かし入れプロセスのあらゆる面にわたって安全性を提供するデジタル映画透かし入れシステムを提供する。
【解決手段】　デジタル画像シーケンスの１つ以上のフレームからなる映画データに、メッセージ・データを表す透かしを安全に埋め込み、および、埋め込まれた透かしを含むデジタル画像シーケンスの１つ以上のフレームを表示するためのシステムと方法は、安全環境を提供すること、透かしを入れた映画データを生成するために、安全環境内で映画データと透かしと組み合わせること、および、安全環境内で、透かしを入れられた映画データから表示された画像を生成することを含んでいる。



【特許請求の範囲】
【請求項１】　デジタル画像シーケンスの１つ以上のフレームからなる映画データに、メッセージ・データを表す透かしを安全に埋め込み、埋め込まれた透かしを含むデジタル画像シーケンスの１つ以上のフレームを表示するシステムであって、
安全な環境を提供するための手段と、
透かしを入れた映画データを生成するために、安全環境内で映画データと透かしと組み合わせるための手段と、安全環境内で、透かしを入れられた映画データから、表示された画像を形成するための手段とを含むことを特徴とするデジタル画像シーケンスの安全透かし入れシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、一般にデジタル画像処理の分野、特に、安全環境内でデジタル画像シーケンスに透かしを埋め込むためのシステムに関する。
【０００２】
【従来の技術】デジタル透かし入れは、所有権を立証し、データの起源を追跡し、無許可のコピーを防ぎ、もしくは、内容に関する付加的情報（メタ・データ）を搬送するような目的で、画像、もしくは画像シーケンスに隠されたメッセージを埋め込むことを意味する。透かしを入れることは、デジタル・スチール・カメラ、デジタル・ビデオ・カメラ、プリンター、および他のハードコピー出力装置、および内容配達サービス（例えばインターネット・ベースの写真仕上げ）を含む、広範囲にわたる製品で、使用される可能性がある。近年、デジタル映画館と呼ばれる、劇場用映画の電子配給と表示において著しい関心がある。スタジオや配給業者には、映画内容を無許可の使用から保護する、強力なニーズがあり、透かし入れは、所有権を立証し、盗まれた内容のソースを辿る（映画配給、および／または、プレゼンテーションの時点で挿入される、隠された日付／時間／場所のスタンプの使用を通して）ことにより、これを援助することができる。本発明は、特に画像シーケンスに透かしを入れることに関連するが、それは、このようにして、デジタル映画館のようなアプリケーションにおいて有用性を持つ。
【０００３】多くの透かしを入れる方法は、特許や技術文献を含む先行技術において記述されている。これらの方法の多くは、ＨａｒｔｕｎｇおよびＫｕｔｔｅｒの、「マルチメディア透かし入れ技術」、Ｐｒｏｃ．ＩＥＥＥ、８７（７）、ｐｐ．１０７９－１１０７（１９９９）、および、Ｗｏｌｆｇａｎｇ他、「デジタル画像およびビデオのための知覚透かし」、Ｐｒｏｃ．ＩＥＥＥ、８７（７）、ｐｐ．１１０８－１１２６（１９９９）のようなレビュー書類に記述されている。
【０００４】様々な方法の根本的相違は、透かしが、空間領域もしくは周波数領域のいずれに適用されるかである。空間領域透かし入れ技術は、透かしパターンを直接デジタル画像のピクセル値に加えるものであり、それに対して、周波数領域透かし入れ技術は、透かしパターンを、デジタル画像を表す変換係数（例えば、ＪＰＥＧおよびＭＰＥＧ－圧縮画像に用いられる、離散的コサイン変換（ＤＣＴ）係数）に加えるものである。先行技術での空間領域技術の例には、Ｈｏｎｓｉｎｇｅｒ他に対して２０００年３月２８日に発行された米国特許第６，０４４，１５６号、およびＲｈｏａｄｓに対して１９９７年６月３日に発行された米国特許第５，６３６，２９２号がある。先行技術での周波数領域技術の例には、Ｇｉｒｏｄ他に対して１９９８年９月１５日に発行された米国特許第５，８０９，１３９号、Ｌｅｅ他に対して１９９９年５月４日に発行された米国特許第５，９０１，１７８号、およびＣｏｘ他に対して１９９９年７月２７日に発行された米国特許第５，９３０，３６９号がある。
【０００５】空間領域アプローチであれ、周波数領域アプローチであれ、大部分の技術は、透かし入れおよび抽出処理に、疑似ランダム・ノイズ（ＰＮ）シーケンス（または複数のシーケンス）を利用している。ＰＮシーケンスは、概してメッセージ・データにより変調されるキャリヤー信号として用いられ、結果としてそれは、多くのピクセルまたは変換係数を横切って分布される分散メッセージ・データ（すなわち、透かしパターン）となる。ＰＮシーケンスを生成する際には、一般にシークレットキー（すなわちシード値）が用いられるが、透かし、およびそれに関係づけられた本来のメッセージ・データを抽出する場合は、このキーを知っていなければならない。デジタル映画システムのために透かしを入れる環境として、その映画が計画中に透かしを埋め込むことが好ましい。これにより、埋め込まれた透かしに、ユニークなプレゼンテーション情報（劇場、特定のスクリーン、タイムスタンプなどを示す）を含めることができる。映画が不法にコピーされた場合、窃盗の時間と場所を示すユニークなプレゼンテーション情報（「指紋」として知られる）は、透かしに含まれた他のあらゆる情報と同様に、コピーに埋め込まれた透かしから抽出することができる。そのような情報が法的手続きで使われる場合、情報がどんな形であれ損なわれていないことを示す必要がある。
【０００６】典型的な映画館では、多くの人々が、映画内容と映写装置にアクセスする可能性がある。これは、劇場のオーナー、映写技師、メンテナンス人員、劇場により雇用されていないが無許可のアクセスが可能な個人をも含む。映画内容を表すデジタル・データへのアクセスは、品質劣化なく簡単にコピーし得るため、これは深刻な問題である。これを防ぐためには、デジタル映画データが、強力な暗号化技術で保護されていなければならないことはよく理解されている。こうした技術では、シ

ークレットキーに、パブリックキー・インフラストラクチャ（ＰＫＩ）に基づくもののような、よく知られたセキュリティ・プロトコルを通して、安全に劇場に届けることが可能な暗号化データの解読を要求する。暗号化、およびセキュリティ・プロトコルの広範な記述は、Ｍｅｎｅｚｅｓ他による、「応用暗号ハンドブック」、ＣＲＣ Ｐｒｅｓｓ，Ｂｏｃａ Ｒａｔｏｎ，ＦＬ，１９９７，ＩＳＢＮ０－８４９３－８５２３－７に見られる。

【０００７】

【発明が解決しようとする課題】デジタル映画データに透かしを入れる場合、透かしを入れるシークレットキーは、透かし入れと抽出に必要な、少なくともある程度の安全性を提供する。透かしキーは、解読キーのために使われるのと同一の安全方式を用いる劇場に、送致することができる。しかしながら、それは、デジタル映画システムで、透かしキー（または、複数のキー）だけを制御するには十分とは言えない。多くの人々が、デジタル映画画像処理システムの様々な構成要素にアクセス可能かもしれないため、透かし入れプロセスの完全な状態が損傷を受けると危惧されるあらゆる潜在的な点に、安全性を提供する必要がある。

【０００８】したがって、このように、埋め込まれた透かしと、それが表す情報の完全性を確保するために、透かし入れプロセスのあらゆる面にわたって安全性を提供する、デジタル映画透かし入れシステムが必要とされている。

【０００９】

【課題を解決するための手段】この要請は、本発明によって満たされるものとなる。本発明は、デジタル画像シーケンスの１つ以上のフレームからなる映画データに、メッセージ・データを表す透かしを安全に埋め込み、さらに、埋め込まれた透かしを含む、デジタル画像シーケンスの、１つ以上のフレームを表示するシステムと方法を提供し、それは安全環境を提供すること；透かしを入れた映画データを作成するために、安全環境内で、映画データと透かしとを組み合わせること；および、安全環境内で、透かしを入れられた映画データから表示画像を形成することを含んでいる。

【００１０】本発明は、こうした透かしに含まれる情報の正当性を確保するために、デジタル画像シーケンスで透かしを埋め込む間、改善された安全性を提供する。また、キーおよび／またはメッセージのような、透かしとして入れられる重要なパラメータを安全に更新すること、およびこれらの更新されたパラメータを安全に記録することを提供する。

【００１１】

【発明の実施の形態】前述のように、秘密の透かしキー（複数の場合もある）は、よく知られた暗号化技術とセキュリティ・プロトコルを用いて、配送の間、保護されることができる。しかしながら、デジタル映画システムでは、強化された安全性を提供するために、および／または透かしパターンの可視性を最小にするために、映画シーケンスでの特定数のフレームが過ぎ、ルート・キーの全部または一部を変えることが好ましいかも知れない（パターンを変化させることは、変化しない透かしパターンより、鑑賞者による認知が難しい）。キーを修正する能力は、ローカルの劇場環境内で、キー生成の少なくとも若干の制御を伴うこともある。キーのそのような修正は、安全な方法でなされなければならず、さらに、後の抽出を実行するためには、安全にキーの使用を探知する必要もあるだろう。

【００１２】しかしながら、デジタル映画システムにおいては、透かしキーを制御するだけでは十分とは言えない。透かしメッセージ・データを保護することもまた、必要である。なぜなら、メッセージ・データが違法コピーから抽出される場合、メッセージ・データのいかなる改竄も、劇場および／または時間を、不正確に識別させる原因になりかねないからである。さらに、特定数フレームの後、時間コードの更新がなされるように、メッセージ・データを修正をすることが好ましいかもしれない。安全にメッセージ使用を探知することも必要であろう。

【００１３】最後に、透かし入れの後、デジタル映画データのために安全性を提供する必要がある。たとえデジタル映画データに、すでにユニークな情報の透かしが入れられているとしても、同様に２次透かし（オリジナルの透かしとは異なる情報を含む）が埋め込まれる可能性もある。どの透かしが最初の透かしであるかを解明することは不可能となることもあり（「行き詰まり」問題）、それは、いかなる法的手続きにおいても、本来の透かしの確実性を打ち砕いてしまう。

【００１４】本発明では、安全性は、安全環境内で透かし入れプロセスを実行することで達成される。安全環境とは、無許可の個人が、意味ある方法で、プロセスの、任意の格納された情報、または、任意の入力、出力、または、内部接続にアクセスすることができないことを意味する。これは、無許可の個人が、透かしを入れるプロセス、およびそのパラメータについての情報を得、および／または、それに影響を与えるのを防ぐ。たとえデータがすでに透かしを埋め込まれている場合であっても、それは、また、映画を表すデジタル・データが獲得されるのを防ぐ。

【００１５】安全な環境は、物理的、および、論理的保護技術を用いることを通して成し遂げられる。簡単な物理的保護技術は、適切なキーまたは組合せだけでしかアクセスできない施錠された部屋に、全てのシステム構成要素と、任意の関連情報を置くことである。同じように、システム構成要素は、（施錠された蓋がある硬化鋼のケースのような）その機械的特性によって、改竄に抵抗する強靭な物理的ハウジングに含まれることができ

た。

【００１６】ハウジングは、また、改竄があった場合、電源を切り、さらに、重要な記録箇所を消去する蓋スイッチ、および他の安全装置を含むことができる。更なる物理的な安全性は、半導体チップのようなハイテクノロジー方法、および、いかなる改竄が起こっても、操作不能となるよう特に設計された回路を用いて提供することができる。これらのハイテクノロジー・セキュリティー処置のいくらかの議論は、Ａｎｄｅｒｓｏｎ他による「タンパー抵抗－訓戒注釈」、Ｔｈｅ Ｓｅｃｏｎｄ ＵＳＥＮＩＸ Ｗｏｒｋｓｈｏｐ ｏｎ Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｍｍｅｒｃｅ Ｐｒｏｃｅｅｄｉｎｇｓ，Ｏａｋｌａｎｄ，ＣＡ，Ｎｏｖ．１９９６，ｐｐ．１－１１，ＩＳＢＮ１－８８０４４６－８３－９に見られる。しかしながら、デジタル映画システムでは、若干の情報が、１つの物理的場所から、別の場所へ転送される必要があるらしく、論理的方法によって、この情報に、適切な保護を与えなければならない。たとえば、映画を表すデジタル・データは、配給サイトから各劇場まで転送されなければならない。そして、前述したように、このデータは、強い暗号化方法とセキュリティ・プロトコルを用いて、保護することができる。

【００１７】安全なデジタル映画透かし入れシステムの基本的構成は、図１に示されている。リモート・データ・サーバ１０（例えば配給サイト）は、圧縮され、暗号化された映画データを劇場へ配送する。映画は、現在の技術の制約の範囲内で、データのより効果的な転送を実現するために圧縮されるが、圧縮は本発明の作用にとって本質的ではない。圧縮データは、劇場への配送の間に、無許可の個人がデジタル映画データにアクセスするのを防ぐために暗号化される。リモート解読キー・サーバ１２は、暗号化された映画データを解読するために、安全な解読キー（または、複数のキー）を劇場に配送する。若干のシステムでは、リモート・データ・サーバ１０、およびリモート解読キー・サーバ１２は、単一のサーバ内に含まれていてもよい。他のシステムでは、リモート・データ・サーバは、映画データを劇場、例えばＤＶＤディスクのような物理的な格納メディア、に配送するために、別の手段で置き換えることができた。

【００１８】劇場で、圧縮され、暗号化されたデータと解読キーは、解読ユニット１４に送られる。解読ユニットは、解読キーを用いて、暗号化されていない圧縮映画データを生成するために、圧縮され、暗号化されたデータを解読する。圧縮された映画データは、それから非圧縮映画データを生成するため、デコンプレッション・ユニット１６に送られる。非圧縮映画データは、デジタル・データの１つ以上のフレームのシーケンスを表す。個々のフレームは、フレームｎとして示される（ｎ＝１，２，．．．，Ｎ）。ここでＮは、映画シーケンスのフレームの総数である。

【００１９】各フレームのための非圧縮デジタル・データは、透かしを含む映画データを生成するために、デジタル映画データを透かしパターンと組み合わせる、透かし入れユニット１８に送られる。以後にすぐに述べられるように、透かしパターンは、多くの異なるアプローチを用いて生成可能であり、特定数のフレームの後、透かしパターンを変化させることも可能である。各フレームに透かしを入れる必要はないかもしれないが、一般に、少なくとも相当数のフレームが、透かしパターンを含むことになる。

【００２０】透かしを入れられた映画データは、それから、デジタル・データを劇場の聴衆による鑑賞可能な可視画像に変える、画像形成アセンブリ２０に送られる。結果は、表示された映画内容の範囲内で埋め込まれた透かしを含む投影フレームｎである。海賊版ビデオ業者が、投影された映画の無許可コピーを制作する場合、透かしはコピーと共に搬送され、違法コピーの場所および時間のような、その映画に関する情報を示すために、後に抽出されることができる。

【００２１】本発明の好ましい実施例では、解読ユニット１４、デコンプレッション・ユニット１６、透かし入れユニット１８、および、画像形成アセンブリ２０は、すべて図１に示される劇場の安全環境内に含まれる。これは無許可の個人が、解読データ、デコンプレスト・データ、もしくは、透かしを入れたデータにアクセスできないことを意味し、さらには、そのような人物が、透かし入れプロセスに関する情報に影響を与えたり、得たりすることができないことを意味する。安全な環境は、「プロジェクター」と一般に呼ばれる、単一の物理ユニットに、これらの処理ユニットの全てを統合することによって提供することができる。プロジェクターは、任意の内部構成要素、もしくは、コネクションへの無許可のアクセスを防ぐための十分な物理的安全方策を含んでいる。これらの方策は、（施錠された鋼のケースのような）抗改竄ハウジング、および／または、全体的なシステムの完全性をモニターし、無許可のアクセスがなされた場合には、構成要素を操作不能にする、侵入－検知回路を含むことができる。透かし入れ、および解読プロセスを保護するために、侵入－検知回路はまた、システムの完全性が危うくされた場合、キーレジスターおよびメッセージ・レジスターのような様々な記録箇所を削除してしまってもよい。

【００２２】今述べられた好ましい実施例では、解読、デコンプレッション、透かし入れ、および、画像形成プロセスは、すべて組み合わされて単一の安全ユニットにされている。しかしながら、これらのプロセスを、安全な論理接続によって接続された、２つ以上の物理ユニットに分けることも有益であろう。図２に示されるように、解読ユニット１４とデコンプレッション・ユニット１６とは、１つの安全な物理ユニットに収容され、一

方、透かし入れユニット１８と画像形成アセンブリ２０は、他の安全な物理ユニットに収容されてもよい。これらの２つの安全ユニットは、安全なローカル・コミュニケーション・リンクを用いて接続され、その安全性は、たとえば、強力な暗号化／デコンプレッション・プロトコルによって提供される。このシステムでは、透かし入れユニット１８と画像形成アセンブリ２０とを含む安全な物理ユニットは、プロジェクターを構成する。また、安全なローカル・コミュニケーション・リンクを伴う安全な物理ユニットの他の構成を組み上げることも可能であり、それは、デコンプレッション・ユニット１６からの、および画像形成アセンブリ２０への、安全なローカル・コミュニケーション・リンクを伴う分離された物理ユニットに透かし入れ装置１８を配置することを含む。

【００２３】図１の安全な透かし入れシステムでは、透かしは、与えられたフレームｎのための非圧縮映画データと組み合わせられる。前述したように、この透かし組合せプロセスは、空間領域または周波数領域においてなされることができる。しかしながら、本発明の他の実施例では、透かし組合せプロセスは、フレームｎのための圧縮データに適用される。ＭＰＥＧとＪＰＥＧのような圧縮技術は、本質的にオリジナル・イメージ・データの周波数分解を含んでおり、従って、それらは、周波数領域透かし入れを実行するための便利なフレームワークを提供することができる。図３は、圧縮データに透かし入れを実行する、安全な透かし入れシステムを示す。このシステムでは、圧縮され、暗号化された映画データは、リモート・データ・サーバ１０から、解読ユニット１４に送られ、リモート解読キー・サーバ１２は、解読ユニットに安全な解読キーを提供する。解読ユニット１４は圧縮映画データを生成し、圧縮映画データはその後、透かしを含む圧縮データを生成するために、透かし入れユニット１８で透かしパターンと組み合わせられる。圧縮され、透かしを入れられたデータは、それからデコンプレッション・ユニット１６に送られ、そこで、透かしを入れられた映画データ、すなわち、透かしを含む非圧縮映画データを生成する。透かしを入れられた映画データは、デジタル・データを、劇場で聴衆が鑑賞可能な可視画像に変換する画像形成アセンブリ２０に送られる。このシステムでは、解読、デコンプレッション、透かし入れ、および、画像生成プロセスは、再び安全環境内に含まれ、それは、単一の安全な物理ユニット、もしくは、安全なコミュニケーション・リンクによって接続された、複数の安全な物理ユニットであり得る。

【００２４】図１－３の安全な透かし入れシステムでは、圧縮され、暗号化されたデータは、リモート・データ・サーバ１０から、解読ユニット１４に直接送られる。これは、映画データのリアルタイム伝送を意味する。多くのシステムでは、後の再生のために、圧縮され、暗号化されたデータを格納するローカル劇場サーバを持つことが望ましい。図４ではこの構成を示しており、ここでは、リモート・データ・サーバ１０は、圧縮され、暗号化されたデータを、ローカル劇場サーバ２２に送り、そこでデータは、後の使用に備えて格納される。圧縮が、本発明にとって必須でない一方で、効率的な格納および映画データの配送のための要請により、それは、多くのシステムで使われている。しかしながら、暗号化は、データを無許可のアクセスから保護するために必要な構成要素であり、それがローカル劇場サーバに保存される場合は、完全に安全な環境とは言えないかもしれない。映画が上映される時、ローカル劇場サーバ２２は、圧縮され、暗号化されたデータを、圧縮された映画データを生成するために解読キーを用いる解読ユニット１４に送る。図１のシステムのために述べたように、圧縮データはデコンプレッション・ユニット１６によってデコンプレスされ、さらに、透かし入り映画データを生成するために、透かし入れ装置１８を用いて、透かしパターンが、デコンプレスされた映画データと組み合わせられる。透かしを入れられた映画データは、その後、透かしを埋め込まれた可視画像を作る、画像形成アセンブリ２０に送られる。再び、解読、デコンプレッション、透かし入れ、および画像形成ユニットは、安全環境内に含まれている。

【００２５】ローカル劇場サーバを、安全環境内に移動させることもまた、有益であろう。図５に示されるように、この構成は、圧縮され、暗号化された映画データを、解読ユニット１４によって解読させ、結果として生じる圧縮映画データは、それからローカル劇場サーバ２２に格納される。ローカル劇場サーバ２２が安全環境内に含まれているので、無許可の個人によるデータへのアクセスが防がれ、圧縮データは、非暗号化形式で格納することができる。映画が発表される時点で、ローカル劇場サーバは、圧縮された映画データを、デコンプレッション・ユニット１６に送り、その結果得られる非圧縮映画データは、それから透かし入れユニット１８により透かしを入れられ、画像形成アセンブリ２０を用いて表示される。また、解読ユニット１４とデコンプレッション・ユニット１６の後、ローカル劇場サーバが配置可能となり得る。その場合には、ローカル劇場サーバ２２は、安全環境内に、解読された、非圧縮映画データを格納する。このシステムは、メモリ必要条件に関しては非能率的である反面、プレゼンテーション時点では、映画データに対する実行処理を単純化する。映画上映ごとに、解読、デコンプレッションを繰り返すよりも、一度にそれをしてしまう方が、遥かに簡単である。

【００２６】今述べられた、図１－５に示される透かし入れシステムでは、透かしパターンは、透かし入れユニット１８が利用できるようにされる。このパターンは、製造の時点で、透かし入れユニットにプリセット可能で、透かし入れユニットおよび／またはプロジェクター

の、ユニークなＩＤを表す情報を含むことができる。しかしながら、このアプローチは非常に制限されたもので、以下のために、透かしパターンを何度も修正することが好ましい：１）透かし情報への追加的な安全性を提供する；２）透かし情報（例えば、タイム・スタンプ情報を反映するために）を更新する；そして、３）劇場聴衆に対する透かしパターンの可視性を最小にする。本発明の他の好ましい実施例では、透かしパターンは、映画フレームのシーケンスの様々な点で、透かしキーおよび／または透かしメッセージを変えることによって修正される。図６に示されるように、プリセットの透かしパターンは、透かしキー生成装置２６から透かしキーを、透かしメッセージ生成装置２８から透かしメッセージを受け取る、透かしパターン生成装置２４によって取り替えられる。透かしパターン生成装置２４、キー生成装置２６、メッセージ生成装置２８、および透かし入れユニット１８は、安全環境内に全て含まれる。前述したように、これらの透かし入れ構成要素のための安全環境は、単一の物理ユニット（これは、例えば、画像形成アセンブリ２０などの、他のシステム構成要素を含んでいてもよい）に構成可能であり、または、透かし入れ構成要素が、物理ユニットの間でデータを搬送する安全なコミュニケーション・リンクを装備した、２つ以上の物理ユニットに存在させられることが可能であった。たとえば、透かしパターン生成装置２４、キー生成装置２６、およびメッセージ生成装置２８は、１つの物理ユニット（劇場にあっても、また、リモート・サイトにあってもよい）に含められることができ、そして、透かし入れ装置１８は、分かれた物理ユニットに含められることができる。

【００２７】透かしキー、および／または、透かしメッセージは、要求があれば、図６に示されるシステムを用いて映画フレームのシーケンスの間中、修正することができる。例えば、透かしキーは、ｍ≧１の場合、ｍフレームごとに変更可能であり、または、キーは、透かしキー生成装置２６の範囲内で、ランダムな方法で変更することもできる。透かしを抽出するためには、キーが判明していなければならないので、限られた数の異なるキーだけを使うことが有益だろう。限られた数のキーを用いて、後の透かし抽出プロセスの間、異なるキーの徹底的な検索を実行することは、簡単である。透かしキーを変えることにより、１つのフレームに使われるキーの知識が、他のフレームに使われるキーについて何の知識も提供しなくなり、透かし入れプロセスに、更なる安全性を提供することになる。加えて、大部分の透かし入れ技術では、異なるキーの使用は、完全に異なる透かしパターンをもたらす。これは、個人が複数フレームを平均する（動きのある画像内容を損なう反面、変化のない透かしパターンを補強する）ことによって、透かしパターンを特定されるのを防ぐ。さらに、時間を通して変わる透かしパターンは、劇場の聴衆の鑑賞者にとり、より見つけられにくい／より不快ではないことになるだろう。

【００２８】同様に、透かしメッセージは、各映画シーケンスの各フレーム、もしくは、シーケンスの範囲内の一定数のフレームごとに変更可能である。特に、透かしメッセージは、時間や日付情報と同様に、例えば、劇場特定スクリーンのユニークなＩＤなど、特定のプレゼンテーション情報を含むように修正可能である。さらに、時間情報を、映画フレームのシーケンスを通して更新することができ、その結果、ｍ≧１の場合、新しいタイム・スタンプが、ｍフレームごとに、透かし情報に含まれるようにすることができる。時間スタンプに十分な正当性を提供するために、透かしメッセージ生成装置２８は、安全環境内で完全なタイムレコーダーを含むことができる。無許可の個人は、映画データ処理経路の中で、１つ以上の必要なコンポーネントを使用不能にすることなくタイムレコーダーを修正することができない。

【００２９】透かしパターン生成装置２４は、透かしキー、もしくは、透かしメッセージが変わる時だけ、新しい透かしパターンを生成する必要がある点に注意を向ける必要がある。透かしパターン生成装置は、それぞれ、透かしキー生成装置２６と、透かしメッセージ生成装置２８で提供される、キー、およびメッセージとをモニターすることができ、キーもしくはメッセージが修正される場合に、新しい透かしパターンが生成される。また、透かしパターン生成装置２４の範囲内で、予め計算して、メモリに格納された、限定数の透かしパターンを用いることが可能である。この場合、透かしキーおよびメッセージは、ルックアップ・テーブルにおけるアドレスの働きをして、対応する透かしパターンがメモリから取り出される。

【００３０】本発明の他の好ましい実施例では、透かしキー生成装置２６で生成される透かしキーと、透かしメッセージ生成装置２８で生成される透かしメッセージは、安全にリモート透かしデータベース３０に転送される。図７に示されるように、透かしキー生成装置２６で生成される透かしキーは、格納して、後日映画データの無許可コピーからの透かし情報抽出の使用に供されるために、リモート透かしデータベース３０へ、安全なコミュニケーション・リンク経由で送られる。安全なコミュニケーション・リンクは、よく知られた暗号化方法とプロトコルを用いて提供することができた。透かしデータベースにおいて、各透かしキーは、所与の映画、および、特定の劇場／スクリーン、および／または、上映からの、特定フレームもしくは複数のフレームに関連している場合がある。しかしながら、それはまた、特定のフレームもしくは複数のフレームとの関連を持たない、特定の劇場／スクリーン、および映画上映のために使われたキー、もしくは複数のキーを記録するだけで十分であるかもしれない。同様に、透かしメッセージ生成装置２

８で生成される透かしメッセージは、安全な手段によって、リモート透かしデータベース３０へ送られ、そこで、特定フレームもしくは一連のフレーム、および／または、特定の劇場／スクリーン、および上映に関係づけることができる。リモート透かしデータベース３０で、透かしキーとメッセージは、暗号化形式で格納されるか、もしくは、データベース自体が、安全環境内に含まれるならば、解読された形式で保存可能である。

【００３１】本発明の好ましいもう１つの実施例では、透かしキーおよび／または透かしメッセージの全部または一部は、リモート透かしサーバで提供される。図８に示されるように、リモート透かしサーバ３２は、安全環境内に存在する透かしキー生成装置２６に、透かしルート・キーを安全に送る。ルート・キーが部分キーに過ぎない場合は、透かしキー生成装置２６は、完全なキーを作るために接尾辞および／または接頭辞を、ルート・キーにつけ加える。あるいは、その後修正されずに透かしパターン生成装置に送られる完全なキーを、リモート・サーバが送ることも可能である。完全なキーもまた、後に透かしキー生成装置２６で修正される初期化キーとして使うことができる。リモート透かしサーバ３２はまた、多くのルート・キーを送ることができ、この場合の各ルート・キーは、映画における特定フレームもしくは複数フレームのシーケンスと関連している。

【００３２】同様に、リモート透かしサーバ３２は、安全環境内に存在する透かしメッセージ生成装置２８に、安全に透かしルート・メッセージを送る。ルート・メッセージは、特定の劇場、および、スクリーンのユニークなＩＤを含み、および／または、映画の特定の上映のためのユニークなプレゼンテーションＩＤを含むことができる。透かしメッセージ生成装置２８は、その後、タイム・スタンプをユニークなＩＤに加えることができた。ここで、タイム・スタンプは、映画を上映する際に、様々な点で更新される。ルート・メッセージは、また、劇場および時間情報を含む完全なメッセージ（もしくは、一連のメッセージ）であることが可能である。

【００３３】透かしルート・キーおよびルート・メッセージの安全性は、転送の間、よく知られた暗号化方法とプロトコルにより提供される。さらに、リモート透かしサーバは、劇場へそれらが配送される前に、無許可の個人がルート・キーもしくはメッセージを改竄するのを防ぐため、安全環境内に保護されている。リモート透かしサーバも、透かしルート・キー、および、ルート・メッセージを特定の映画フレームもしくは一連のフレーム、および／または、特定の劇場／スクリーン、および、上映と関連させる、安全なデータベースを維持している。

【図面の簡単な説明】

【図１】　デジタル映画システムにおいて、安全環境内で映画データに透かしを埋め込むためのシステムを示す図である。

【図２】　デジタル映画システムにおいて、安全環境内で映画データに透かしを埋め込むための代わりのシステムを示す図である。

【図３】　デジタル映画システムにおいて、安全環境内で圧縮した映画データに透かしを埋め込むためのシステムを示す図である。

【図４】　暗号化されたデータおよび圧縮されたデータのローカル・ストレージを伴うデジタル映画システムにおいて、安全環境内で、透かしを埋め込むためのシステムを示す図である。

【図５】　暗号化されたデータおよび圧縮されたデータのローカル・ストレージを伴うデジタル映画システムにおいて、安全環境内で、透かしを埋め込むためのシステムを示す図である。

【図６】　ローカルに生成された透かしキーおよび透かしメッセージを用いるデジタル映画システムにおいて、安全環境内で、透かしを埋め込むためのシステムを示す図である。

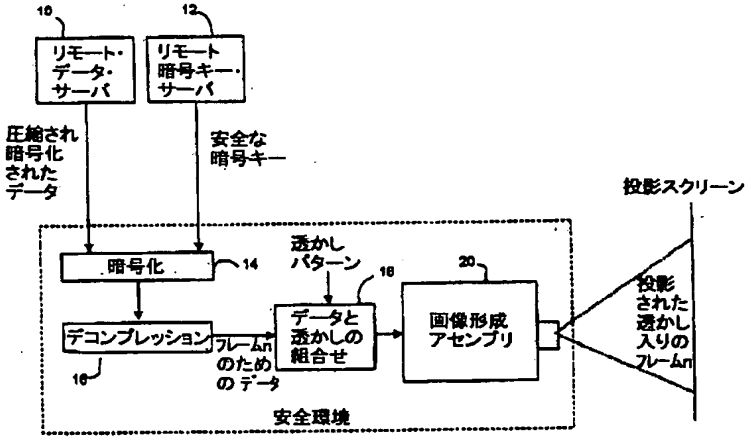
【図７】　ローカルに生成された透かしキーおよび透かしメッセージのリモート・データベース・ストレージを伴うデジタル映画システムにおいて、安全環境内で、透かしを埋め込むためのシステムを示す図である。

【図８】　リモート透かしサーバで生成される安全な透かしルート・キーおよび透かしルート・メッセージを用いるデジタル映画システムにおいて、安全環境内で、透かしを埋め込むためのシステムを示す図である。

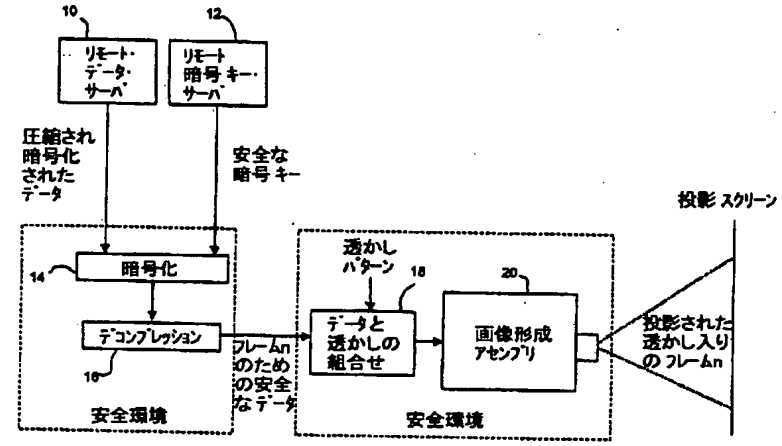
【符号の説明】

１０　リモート・データ・サーバ、１２　リモート解読キー・サーバ、１４解読ユニット、１６　デコンプレッション・ユニット、１８　透かし入れユニット、２０　画像形成アセンブリ、２２　ローカル劇場サーバ、２４　透かし入れパターン生成装置、２６　透かし入れキー生成装置、２８　透かし入れメッセージ生成装置、３０　リモート透かしデータベース、３２　リモート透かしサーバ。

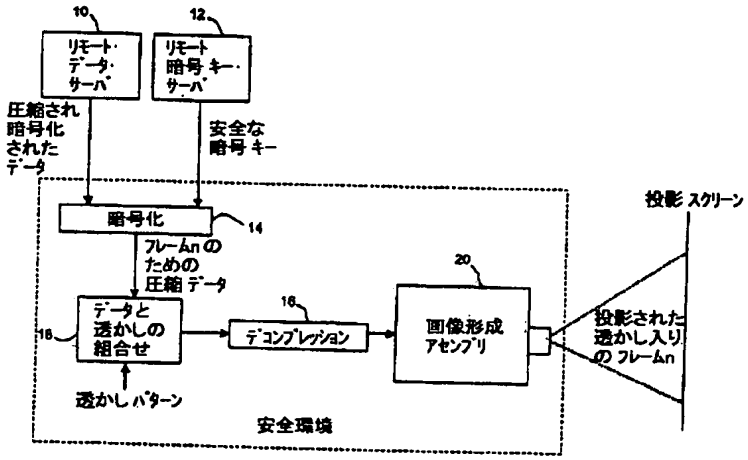
【図１】


10
12
リモート・データ・サーバ
リモート暗号キー・サーバ
圧縮され暗号化されたデータ
安全な暗号キー
投影スクリーン
暗号化
14
透かしパターン
18
20
デコンプレッション
16
フレームnのためのデータ
データと透かしの組合せ
画像形成アセンブリ
投影された透かし入りのフレームn
安全環境

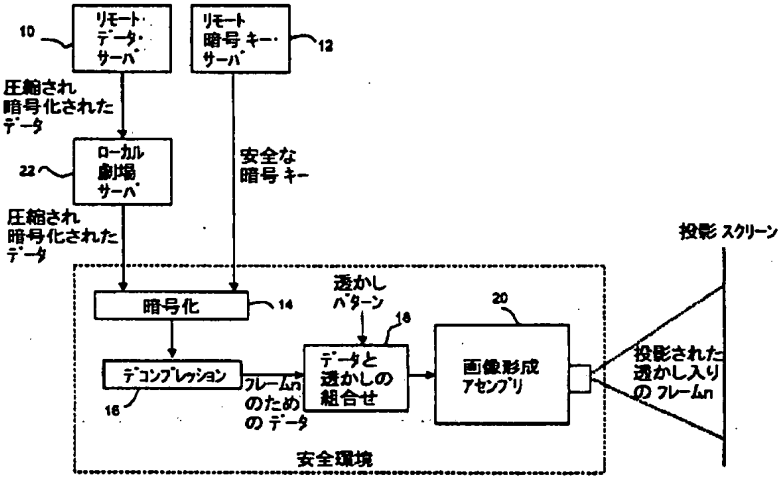
【図２】


10
12
リモート・データ・サーバ
リモート暗号キー・サーバ
圧縮され暗号化されたデータ
安全な暗号キー
投影スクリーン
14
暗号化
デコンプレッション
16
フレームnのための安全なデータ
安全環境
透かしパターン
18
20
データと透かしの組合せ
画像形成アセンブリ
投影された透かし入りのフレームn
安全環境

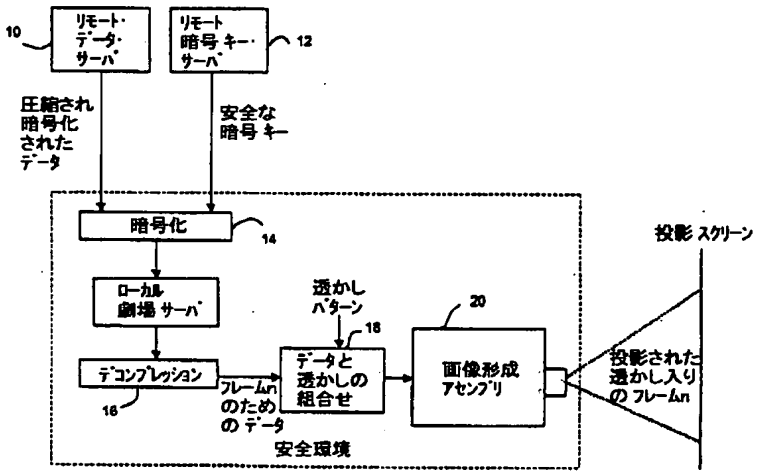
【図３】


10
12
リモート・データ・サーバ
リモート暗号キー・サーバ
圧縮され暗号化されたデータ
安全な暗号キー
投影スクリーン
暗号化
14
フレームnのための圧縮データ
16
データと透かしの組合せ
18
透かしパターン
デコンプレッション
20
画像形成アセンブリ
投影された透かし入りのフレームn
安全環境

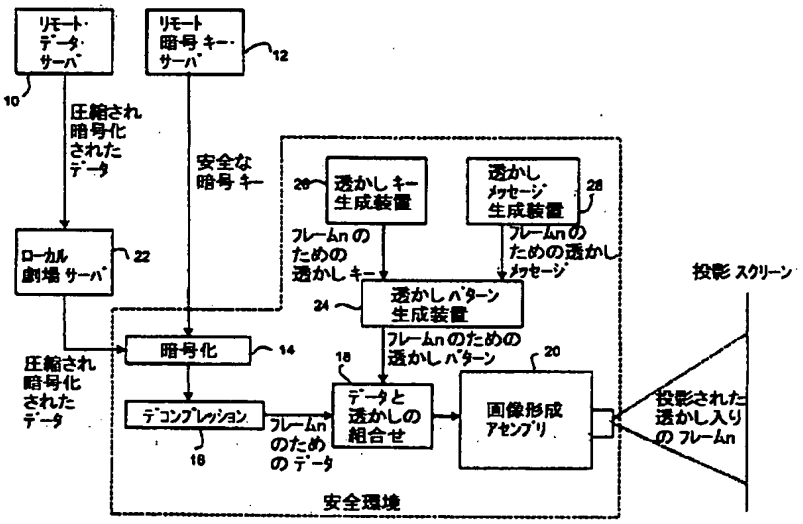
【図４】


10
リモート・データ・サーバ
リモート暗号キー・サーバ
12
圧縮され暗号化されたデータ
22
ローカル劇場サーバ
安全な暗号キー
圧縮され暗号化されたデータ
投影スクリーン
暗号化
14
透かしパターン
18
20
デコンプレッション
16
フレームnのためのデータ
データと透かしの組合せ
画像形成アセンブリ
投影された透かし入りのフレームn
安全環境

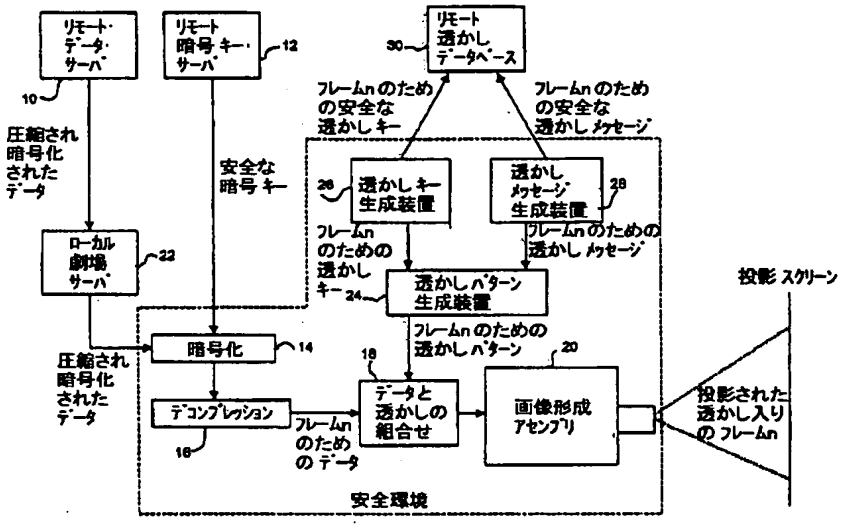
【図５】


10
リモート・データ・サーバ
リモート暗号キー・サーバ
12
圧縮され暗号化されたデータ
安全な暗号キー
暗号化
14
投影スクリーン
ローカル劇場サーバ
透かしパターン
18
20
デコンプレッション
16
フレームnのためのデータ
データと透かしの組合せ
画像形成アセンブリ
投影された透かし入りのフレームn
安全環境

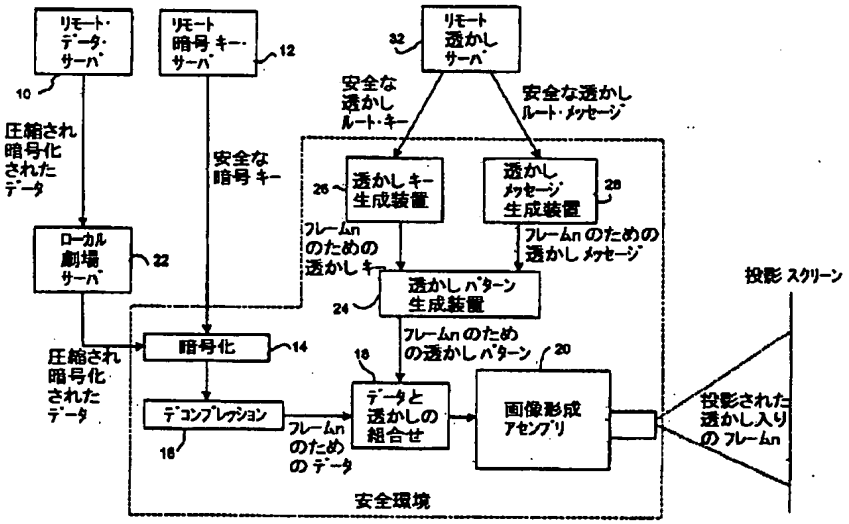
【図６】


リモート・データ・サーバ
10
リモート暗号キー・サーバ
12
圧縮され暗号化されたデータ
安全な暗号キー
透かしキー生成装置
26
透かしメッセージ生成装置
28
フレームnのための透かしキー
フレームnのための透かしメッセージ
ローカル劇場サーバ
22
透かしパターン生成装置
24
フレームnのための透かしパターン
投影スクリーン
暗号化
14
18
20
圧縮され暗号化されたデータ
デコンプレッション
16
フレームnのためのデータ
データと透かしの組合せ
画像形成アセンブリ
投影された透かし入りのフレームn
安全環境

【図７】


リモート・データ・サーバ
10
リモート暗号キー・サーバ
12
リモート透かしデータベース
30
フレームnのための安全な透かしキー
フレームnのための安全な透かしメッセージ
圧縮され暗号化されたデータ
安全な暗号キー
透かしキー生成装置
26
透かしメッセージ生成装置
28
ローカル劇場サーバ
22
フレームnのための透かしキー
フレームnのための透かしメッセージ
透かしパターン生成装置
24
投影スクリーン
暗号化
14
フレームnのための透かしパターン
18
20
圧縮され暗号化されたデータ
デコンプレッション
16
フレームnのためのデータ
データと透かしの組合せ
画像形成アセンブリ
投影された透かし入りのフレームn
安全環境

【図８】


リモート・データ・サーバ
10
リモート暗号キー・サーバ
12
リモート透かしサーバ
32
安全な透かしルート・キー
安全な透かしルート・メッセージ
圧縮され暗号化されたデータ
安全な暗号キー
透かしキー生成装置
26
透かしメッセージ生成装置
28
ローカル劇場サーバ
22
フレームnのための透かしキー
フレームnのための透かしメッセージ
透かしパターン生成装置
24
投影スクリーン
圧縮され暗号化されたデータ
暗号化
14
フレームnのための透かしパターン
20
18
データと透かしの組合せ
デコンプレッション
16
フレームnのためのデータ
画像形成アセンブリ
投影された透かし入りのフレームn
安全環境